APPROVED
by Decision of 21 May 2025
of the Board of Directors of
NEO Finance AB

BUSINESS CONTINUITY PLAN

TABLE OF CONTENTS

GENERAL PROVISIONS

The Business Continuity Plan (the 'Plan') of NEO Finance AB (the 'Company') outlines the measures and procedures implemented by the Company to ensure that the Company's operations are ongoing and uninterrupted, and that the performance of contractual obligations in unforeseen circumstances proceeds without disruption.

The Business Continuity Plan serves as a blueprint for achieving timely and structured operational continuity, or rapid recovery of operations following an emergency. This process includes methods and measures to ensure that the Company's core activities remain stable and uninterrupted both during and after an emergency.

The Plan shall be tested regularly, at least once a year, to ensure the Company's ability to continue its operations and limit losses should operations be disrupted. Any difficulties or disruptions in the testing environment shall be documented and assessed, resulting in appropriate adjustments to the Business Continuity Plan.

The Company's Director or his authorised Deputy Administrator shall be responsible for the implementation of the Plan. Should the Company's Director find himself unable to perform his duties for legitimate reasons (e.g. annual leave, illness, etc.), he shall appoint in advance a Company employee who shall be responsible for performing all duties set out in this Plan.

The Company's Board of Directors shall review and examine the Plan at least once a year or as necessary.

TERMS AND DEFINITIONS

OBD – Open Banking Department of Neopay.

LC – Law on Companies of the Republic of Lithuania.

Shareholder – ERA Capital UAB, company code 300638657, registered office at Ulonų g. 5, Vilnius. The Shareholder holds the majority of the Company's shares.

AML – Prevention of money laundering, terrorist financing and fraud.

GDPR (General Data Protection Regulation) – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

Company – NEO Finance AB, company code 303225546, registered office at Ukmergės g. 126, Vilnius. The Company operates as an Electronic Money Institution, Consumer Credit Provider and Peer-to-Peer Lending Platform Operator.

Subsidiary – Finomark UAB, company code 305538582, registered office at Ukmergės g. 126, Vilnius. The Subsidiary operates as a Crowdfunding Platform Operator.

Companies – The Company and the Subsidiary of the Company.

Crisis Management Group – An ad hoc corporate body responsible for decision-making when an incident or crisis affects all of the Company's operations. This Group is informal and formed at the discretion of the Companies' Management.

EMI – Electronic Money Institution, as defined by the Law on Electronic Money and Electronic Money Institutions of the Republic of Lithuania.

Finomark – A System managed by the Subsidiary, which stores and maintains all data related to the activities of the Peer-to-Peer Lending Operator. The System is available to the customers of the Subsidiary online at https://www.finomark.lt/.

Incident – Any existing or imminent situation that may have a disruptive effect on the normal operations of the Companies and adversely affect the delivery of services. From a business continuity perspective, any Incident may evolve into a crisis if the impact is significant or long-lasting.

Customer – Any natural or legal person using at least one System.

KYB – Due diligence process for business customers (legal persons).

KYC – Due diligence process for individual customers (natural persons).

Licence – Electronic Money Institution Licence No 7 issued to the Company by the Bank of Lithuania on 5 January 2017 (Licence renewed on 30 October 2018 – authorisation to provide payment initiation services; and on 14 May 2020 – authorisation to provide account information services).

PIS – Payment Initiation Service, as defined in the Law on Payments of the Republic of Lithuania.

Neopay – A System for providing PIS/AIS and other open banking services, available online at https://mano.neopay.lt.

Lender – A natural or legal person lending through the System as defined by the LCC.

Supervisory Authority – The Bank of Lithuania and/or other institution of the Republic of Lithuania performing regulatory supervision of the Company.

Paskolų Klubas – A System managed by the Company, which stores and maintains all data related to the Company's electronic money issuance activities, peer-to-peer lending operator activities, and payment services, except for payment initiation and account information services. The System is available to the Company's customers online at https://www.paskoluklubas.lt/prisijungti.

Risk Officer – A person responsible for developing internal risk management models and overseeing the Company's overall risk management system.

AIS – Account Information Service, as defined by the Law on Payments of the Republic of Lithuania.

CPO – Crowdfunding Platform Operator

System – The Paskolų Klubas Peer-to-Peer Lending Platform System, the Finomark Crowdfunding Platform System, the Electronic Money and Payment System, and the Neopay PIS/AIS System, hereinafter collectively referred to as the Systems.

P2PLPO – Peer-to-Peer Lending Platform Operator, as defined by the LCC.

Business Continuity Disruption/Crisis – An unexpected and unwelcome disruption to the Companies' operations in a particular area that may disrupt or cease the Companies' operations and business continuity, i.e. any non-standard situation that poses a risk. This typically begins as an Incident.

CC – Consumer Credit as defined by the LCC.

CCP – Consumer Credit Provider.

CCR – Consumer Credit Recipient, when CC is granted through the System as defined by the LCC.

LCC – Law on Consumer Credit of the Republic of Lithuania.

CISO (Chief Information Security Officer) – A person responsible for managing information and communication technology (ICT) as well as security risks.

All terms used in the singular in this Plan may, where the context so requires, be interpreted as including the plural, and vice versa.

OPERATIONAL RISKS

The core elements of the Business Continuity Plan are as follows:

- Identification of critical business activities;
- Identification of general risks;
- Business impact analysis for each risk;
- Assessment of existing controls and determination of residual risk;
- Planning of required control measures.

The Company's objective is to ensure that the availability of financial or regulated services is not interrupted for more than 2 hours or beyond other contractual or regulatory limits.

The Company's losses are measured in euros when it is necessary to cover the losses incurred, restore the Company's infrastructure, reputation and other conditions to their previous levels.

CRITICAL ACTIVITIES AND SUPPORT RESOURCES

The Companies have identified the following critical activities that fall within the scope of this Plan:

- Electronic Money Institution activities;
- PIS;
- AIS;
- Peer-to-Peer Lending Platform Operator activities;

- Crowdfunding Platform Operator activities;
- Consumer Credit Provider activities.

1. The functions are supported by these resources and providers: [CONFIDENTIAL].
2. Electronic Money Institution activities / Peer-to-Peer Lending Platform Operator activities / Consumer Credit Provider activities: [CONFIDENTIAL].
3. Crowdfunding Platform Operator activities: [CONFIDENTIAL].

RISK SCENARIOS

The Companies have identified and continue to assess the following general risks that may have a negative impact on the continuity of their operations:

- Geopolitical Risk
- Natural Disasters
- Data Centre Failure/Loss
    - A data centre failure can be attributed to cyber-attacks, malicious activity, DDoS attacks, etc.
- Data Transmission Disruptions
    - Data transmission disruptions can be attributed to massive failures that would not only impact the Company, but also lead to major implications. This could also be linked to communication provider outages and DDoS attacks.
- Power Cuts
- Unavailability of Staff
- Equipment Loss or Failure
- Neopay System Loss
    - System loss can occur in a number of scenarios, including cyber-attacks, risks, failures, etc.
- Paskolų Klubas System Loss
    - System loss can occur in a number of scenarios, including cyber-attacks, risks, failures, etc.
- Finomark System Loss
    - System loss can occur in a number of scenarios, including cyber-attacks, risks, failures, etc.
- Neopay System Programming Error/Failure
- Paskolų Klubas System Programming Error/Failure
- Finomark System Programming Error/Failure
- Loss of Access to Office Premises
- Neopay Database Loss
    - Database loss can occur in a number of scenarios, including cyber-attacks, risks, failures, malicious activity, etc.
- Paskolų Klubas Database Loss
    - Database loss can occur in a number of scenarios, including cyber-attacks, risks, failures, malicious activity, etc.
- Finomark Database Loss
    - Database loss can occur in a number of scenarios, including cyber-attacks, risks, failures, malicious activity, etc.
- AML Provider Disruptions
- KYC / KYB Provider Disruptions
- Disruptions or Withdrawal of Other Critical Service Providers

BUSINESS IMPACT ANALYSIS METHODOLOGY

In developing a plan for business continuity, the Company assesses and analyses the impact of a possible risk scenario on the Company's business processes. Business processes should be assessed in terms of:

- The potential impact on finances and reputation;
- How critical business processes are, taking into account the impact values for ensuring the relevant business process;
- Recovery Time Objective (RTO) and Recovery Point Objective (RPO) specified for IT systems and data that are necessary for maintaining business processes;
- The current preparedness of the Companies to operate in unforeseen circumstances;

- The organisational and technological requirements necessary to restore the Companies' operations and information technology activities;
- The methodology described below for assessing how critical business processes are.

Tables 1 and 2. Business Process Impact Classification Values (Qualitative and Quantitative)

Impact Table					
		Low	**Medium Low**	**Medium High**	**High**
Financial Impact, EUR		<20 000	20 000 – 50 000	50 000 – 100 000	>100 000
Customer Attrition		<5%	5% – 20%	20% – 30%	>30%
Impact on Reputation		Risk of negative comments in local low-key media. Negative comments on social media.	Factual negative comments in local low-key media. Negative posts on social media.	Individual press releases in established media, negative content from influencers on social media. There is a risk of recurrence.	Coordinated, widespread and recurring critical coverage of a specific related event. Supported by negative comments from influencers, experts or regulators.
Unavailability of Staff	**Management**	<10%	10% – 20%	20% – 30%	>30%
	Non-management	<10%	10% – 20%	20% – 30%	>30%
Regulatory Impact		No impact.	Warning, bad publicity about a legal violation, inspection.	Fine, warning and disclosure of a legal violation.	Loss of licences, fines. GDPR fines. Removal from payment schemes.
IT Infrastructure		Minor errors.	Loss of the majority of workstations. Loss of knowledge base. Major disruption lasting less than 24 hours.	Partial loss or breach of financial or personal data. Major disruption lasting less than 72 hours.	Significant loss or breach of financial or personal data. Major disruption lasting more than 72 hours.

Probability Table				
	Low	**Medium Low**	**Medium High**	**High**
Probability	Unlikely to happen	Reasonable likelihood of occurrence	Likely to happen	Almost certain to occur
Inherent Risk	The source of risk is unmotivated and it is unlikely that the risk will materialise.	The source of risk is either unmotivated or it is unlikely that the risk will materialise.	The source of risk is either motivated or the risk is naturally expected to materialise.	The source of risk is motivated and the risk may naturally materialise.
Control Measures	Several levels of combined technical and administrative controls in place. Control measures are regularly reviewed and tested.	More than two technical and administrative controls in place. Technical and administrative controls are coordinated to effective levels.	Two technical control measures or a single set of technical and administrative control measures in place.	No risk-mitigating controls in place.

Table 3. The criticality value of a process is calculated by multiplying the impact and probability values. Process criticality scores (quantitative and qualitative):

		Probability			
		L	ML	MH	H
Impact	H	MH	MH	H	H
	MH	ML	ML	MH	H
	ML	L	ML	ML	MH
	L	L	L	ML	MH

The value of L is 1; ML = 2; MH = 3; H = 4. For example, L x H = 1 x 4 = 4.

BUSINESS IMPACT ANALYSIS

Business Impact Analysis				
Core Function	**Scenario**	**Impact**	**Probability**	**Risk**
Geopolitical Risk				
PIS	Geopolitical events disrupt PIS operations. Panic sets in and PIS services are disrupted. This scenario is unlikely because the activity is automated with minimal human intervention. Additionally, geopolitical unrest would likely render PIS activities largely irrelevant.	ML	L	L
AIS	Geopolitical events disrupt AIS operations. Panic sets in and AIS services are disrupted. This scenario is unlikely because the activity is automated with minimal human intervention. Additionally, geopolitical unrest would likely render AIS activities largely irrelevant.	ML	L	L
P2PLPO Activities CPO Activities CCP Activities	It is likely that lending would be restricted during periods of geopolitical unrest.	ML	L	L
EMI Activities	Geopolitical events disrupt CENTROlink operations. This scenario is unlikely because the activity is automated with minimal human intervention. It is expected that the Bank of Lithuania has planned for the continuity of CENTROlink's operations in a secure area and that the provision of services would not be disrupted.	ML	L	L
AML Compliance	Geopolitical unrest leads to an increase in the number of sanctioned individuals and instances of fraud, while the scope of sanctions expands, potentially causing AML disruptions that could have a negative impact on the organisation's reputation, finances, etc.	MH	MH	MH
KYC / KYB	It is likely that geopolitical unrest would lead to a decline in the number of applications from new customers.	ML	L	L
Natural Disasters				
PIS	It is unlikely that natural disasters would disrupt the functioning of payment services and data centres in the Republic of Lithuania.	ML	L	L
AIS	It is unlikely that natural disasters would disrupt the functioning of payment services and data	ML	L	L

Business Impact Analysis				
Core Function	**Scenario**	**Impact**	**Probability**	**Risk**
	centres in the Republic of Lithuania.			
P2PLPO Activities CPO Activities CCP Activities	It is unlikely that natural disasters would disrupt the functioning of payment services and data centres in the Republic of Lithuania.	L	L	L
EMI Activities	It is unlikely that natural disasters would disrupt the functioning of payment services and data centres in the Republic of Lithuania.	L	L	L
AML Compliance	It is unlikely that natural disasters would disrupt the functioning of payment services and data centres in the Republic of Lithuania.	L	L	L
KYC / KYB	It is unlikely that natural disasters would disrupt the functioning of payment services and data centres in the Republic of Lithuania.	L	L	L
Data Centre Failure/Loss				
PIS	PIS service is operated from a single data centre, but backups can be restored extremely quickly from a second location. Data loss would not disrupt the service.	MH	L	ML
AIS	AIS service is operated from a single data centre, but backups can be restored extremely quickly from a second location. Data loss would not disrupt the service.	MH	L	ML
P2PLPO Activities CPO Activities CCP Activities	The systems operate in a Tier 3 Design certified [CONFIDENTIAL] data centre. Backup copies are stored in a remote data centre. This kind of disruption would have a major financial and reputational impact. Data loss can also have a significant impact.	MH	L	ML
EMI Activities	The systems operate in a Tier 3 Design certified [CONFIDENTIAL] data centre. Backup copies are stored in a remote data centre. This kind of disruption would have a major financial and reputational impact. Data loss can also have a significant impact.	MH	L	ML
AML Compliance	AML compliance is outsourced to a third party that ensures continuity of service. It is expected that in the event of a single data centre failure, a backup site would take over. A complete failure would result in payment services being disrupted.	ML	L	L

Business Impact Analysis				
Core Function	**Scenario**	**Impact**	**Probability**	**Risk**
KYC / KYB	KYC/KYB is outsourced to a third party that ensures continuity of service. It is expected that in the event of a single data centre failure, a backup site would take over. A complete failure would result in the inability to authenticate new customers.	L	L	L
Data Transmission Disruptions				
PIS	This scenario is unlikely due to the data centre using different communication providers. A long-term disruption would not have a significant impact, as it would likely constitute a national incident.	L	L	L
AIS	This scenario is unlikely due to the data centre using different communication providers. A long-term disruption would not have a significant impact, as it would likely constitute a national incident.	L	L	L
P2PLPO Activities CPO Activities CCP Activities	This scenario is unlikely due to the data centre using different communication providers. A long-term disruption would not have a significant impact, as it would likely constitute a national incident.	L	L	L
EMI Activities	This scenario is unlikely due to the data centre using different communication providers. A long-term disruption would not have a significant impact, as it would likely constitute a national incident.	L	L	L
AML Compliance	This scenario is unlikely due to the data centre using different communication providers. A long-term disruption would suspend the delivery of other financial services.	ML	ML	ML
KYC / KYB	This scenario is unlikely due to the data centre using different communication providers. A long-term disruption would not have a significant impact, as it would likely constitute a national incident.	L	L	L
Power Cuts				
PIS	This scenario is unlikely due to the data centre's backup power sources. A long-term disruption would not have a significant impact, as it would likely constitute a national incident.	ML	L	L

Business Impact Analysis				
Core Function	**Scenario**	**Impact**	**Probability**	**Risk**
AIS	This scenario is unlikely due to the data centre's backup power sources. A long-term disruption would not have a significant impact, as it would likely constitute a national incident.	ML	L	L
P2PLPO Activities CPO Activities CCP Activities	This scenario is unlikely due to the data centre's backup power sources. A long-term disruption would not have a significant impact, as it would likely constitute a national incident.	ML	L	L
EMI Activities	This scenario is unlikely due to the data centre's backup power sources. A long-term disruption would not have a significant impact, as it would likely constitute a national incident.	ML	L	L
AML Compliance	This scenario is unlikely due to the data centre's backup power sources. A long-term disruption would not have a significant impact, as it would likely constitute a national incident.	ML	L	L
KYC / KYB	This scenario is unlikely due to the data centre's backup power sources. A long-term disruption would not have a significant impact, as it would likely constitute a national incident.	ML	L	L
Unavailability of Staff				
PIS	PIS operation is automated, so unavailability of staff would not cause sudden or significant consequences.	ML	L	L
AIS	AIS operation is automated, so unavailability of staff would not cause sudden or significant consequences.	ML	L	L
P2PLPO Activities CPO Activities CCP Activities	Lending is a semi-automated and standardised process. Limited unavailability of staff is easily mitigated and would not cause significant disruption or loss.	ML	L	L
EMI Activities	EMI activities are automated and standardised. Limited unavailability of staff is easily mitigated and would not cause significant disruption or loss.	ML	L	L
AML Compliance	The AML function is semi-automated, and unavailability of staff would not cause sudden or significant consequences.	ML	L	L
KYC / KYB	The KYC/KYB function is semi-automated, and unavailability of staff would not cause sudden	ML	L	L

Business Impact Analysis				
Core Function	**Scenario**	**Impact**	**Probability**	**Risk**
	or significant consequences.			
Equipment Loss or Failure				
PIS	Any loss of equipment would not affect the service, as it operates in a virtual environment. In the event of a data centre equipment disruption, the PIS operation could be quickly restored.	ML	L	L
AIS	Any loss of equipment would not affect the service, as it operates in a virtual environment. In the event of a data centre equipment disruption, the AIS operation could be quickly restored.	ML	L	L
P2PLPO Activities CPO Activities CCP Activities	Equipment failure in a data centre may cause a disruption that would be slow to recover due to monolithic infrastructure. Infrequent database replication can result in significant data loss and reputational damage.	MH	ML	ML
EMI Activities	Equipment failure in a data centre may cause a disruption that would be slow to recover due to monolithic infrastructure. Infrequent database replication can result in significant data loss and reputational damage.	MH	ML	ML
AML Compliance	It is expected that the loss of equipment would not affect the service because it operates in a virtual environment configured in mirrored mode.	ML	L	L
KYC / KYB	It is expected that the loss of equipment would not affect the service because it operates in a virtual environment configured in mirrored mode.	ML	L	L
Neopay System Loss				
PIS	Complete disruption of service. Regulatory and commercial sanctions.	MH	L	ML
AIS	Complete disruption of service. Regulatory and commercial sanctions.	MH	L	ML
P2PLPO Activities CPO Activities CCP Activities	No impact.	L	L	L

Business Impact Analysis				
Core Function	**Scenario**	**Impact**	**Probability**	**Risk**
EMI Activities	No impact.	L	L	L
AML Compliance	No impact.	L	L	L
KYC / KYB	No impact.	L	L	L
Paskolų Klubas System Loss				
PIS	Complete disruption of service. Regulatory and commercial sanctions. Loss of transaction and contract records, leading to potential losses.	MH	L	ML
AIS	Complete disruption of service. Regulatory and commercial sanctions. Loss of transaction and contract records, leading to potential losses.	MH	L	ML
P2PLPO Activities CPO Activities CCP Activities	Complete disruption of service. Regulatory and commercial sanctions. Loss of transaction and contract records, leading to potential losses.	MH	L	ML
EMI Activities	Complete disruption of service. Regulatory and commercial sanctions. Loss of transaction and contract records, leading to potential losses.	MH	L	ML
AML Compliance	Complete disruption of service. Regulatory and commercial sanctions. Loss of transaction and contract records, leading to potential losses.	MH	L	ML
KYC / KYB	Complete disruption of service. Regulatory and commercial sanctions. Loss of transaction and contract records, leading to potential losses.	MH	L	ML
Finomark System Loss				
PIS	No impact.	L	L	L
AIS	No impact.	L	L	L
P2PLPO Activities	Complete disruption of CPO service. Regulatory and commercial sanctions. Loss of transaction	MH	L	ML

Business Impact Analysis				
Core Function	**Scenario**	**Impact**	**Probability**	**Risk**
CPO Activities CCP Activities	and contract records, leading to potential losses.			
EMI Activities	No impact.	L	L	L
AML Compliance	No impact.	L	L	L
KYC / KYB	No impact.	L	L	L
Neopay System Programming Error/Failure				
PIS	Possible short-term service disruption, notifications to the Bank of Lithuania, reputational damage, contract termination in critical cases.	MH	L	ML
AIS	Possible short-term service disruption, notifications to the Bank of Lithuania, reputational damage, contract termination in critical cases.	MH	L	ML
P2PLPO Activities CPO Activities CCP Activities	No impact.	L	L	L
EMI Activities	No impact.	L	L	L
AML Compliance	No impact.	L	L	L
KYC / KYB	No impact.	L	L	L
Paskolų Klubas System Programming Error/Failure				
PIS	Possible service disruption, sanctions checks on transactions. This may result in reputational or regulatory impact. Possible direct loss of funds.	MH	ML	ML
AIS	Possible service disruption, sanctions checks on transactions. This may result in reputational or regulatory impact. Possible direct loss of funds.	MH	ML	ML

Business Impact Analysis				
Core Function	**Scenario**	**Impact**	**Probability**	**Risk**
P2PLPO Activities CPO Activities CCP Activities	Possible service disruption, sanctions checks on transactions. This may result in reputational or regulatory impact. Possible direct loss of funds.	MH	ML	ML
EMI Activities	Possible service disruption, sanctions checks on transactions. This may result in reputational or regulatory impact. Possible direct loss of funds.	MH	ML	ML
AML Compliance	Possible service disruption, sanctions checks on transactions. This may result in reputational or regulatory impact.	MH	ML	ML
KYC / KYB	Possible service disruption, sanctions checks on transactions. This may result in reputational or regulatory impact.	MH	ML	ML
Finomark System Programming Error/Failure				
PIS	No impact.	L	L	L
AIS	No impact.	L	L	L
P2PLPO Activities CPO Activities CCP Activities	Possible disruption of CPO services. This may result in reputational or regulatory impact.	MH	ML	ML
EMI Activities	No impact.	L	L	L
AML Compliance	No impact.	L	L	L
KYC / KYB	No impact.	L	L	L
Loss of Access to Office Premises				
PIS	No impact.	L	L	L
AIS	No impact.	L	L	L

Business Impact Analysis				
Core Function	**Scenario**	**Impact**	**Probability**	**Risk**
P2PLPO Activities CPO Activities CCP Activities	No impact.	L	L	L
EMI Activities	No impact.	L	L	L
AML Compliance	No impact.	L	L	L
KYC / KYB	No impact.	L	L	L
Neopay Database Loss				
PIS	No impact.	L	L	L
AIS	No impact.	L	L	L
P2PLPO Activities CPO Activities CCP Activities	No impact.	L	L	L
EMI Activities	No impact.	L	L	L
AML Compliance	No impact.	L	L	L
KYC / KYB	No impact.	L	L	L
Paskolų Klubas Database Loss				
PIS	No impact.	L	L	L
AIS	No impact.	L	L	L
P2PLPO Activities CPO Activities	Loss of financial records, complete service disruption, regulatory and financial losses.	H	M	MH

Business Impact Analysis				
Core Function	**Scenario**	**Impact**	**Probability**	**Risk**
CCP Activities				
EMI Activities	Loss of financial records, complete service disruption, regulatory and financial losses.	H	M	MH
AML Compliance	Potential negative impact due to minor non-conformity. It is expected that the provider maintains parallel data storage.	ML	L	L
KYC / KYB	Potential negative impact due to minor non-conformity. It is expected that the provider maintains parallel data storage.	L	L	L
Finomark Database Loss				
PIS	No impact.	L	L	L
AIS	No impact.	L	L	L
P2PLPO Activities CPO Activities CCP Activities	Loss of CPO financial records, complete service disruption, regulatory and financial losses.	H	M	MH
EMI Activities	No impact.	L	L	L
AML Compliance	No impact.	L	L	L
KYC / KYB	No impact.	L	L	L
AML Provider Disruptions				
PIS	Service disruption, possible non-compliance and regulatory consequences.	ML	ML	ML
AIS	No impact.	L	L	L
P2PLPO Activities CPO Activities	Service disruption, possible non-compliance and regulatory consequences.	MH	ML	ML

Business Impact Analysis				
Core Function	**Scenario**	**Impact**	**Probability**	**Risk**
CCP Activities				
EMI Activities	Service disruption, possible non-compliance and regulatory consequences.	MH	ML	ML
AML Compliance	Service disruption resulting in a chain reaction. Potential regulatory and reputational impact.	MH	ML	ML
KYC / KYB	Service disruption, possible non-compliance and regulatory consequences.	ML	ML	ML
KYC / KYB Provider Disruptions				
PIS	No impact.	L	L	L
AIS	No impact.	L	L	L
P2PLPO Activities CPO Activities CCP Activities	Minor disruption.	ML	L	L
EMI Activities	Minor disruption..	ML	L	L
AML Compliance	KYC disruption may lead to inadequate AML compliance and very limited enforcement of sanctions.	ML	L	L
KYC / KYB	Functionality is disrupted, leading to the inability to create relationships with new customers and triggering a chain reaction.	ML	L	L
Disruptions or Withdrawal of Other Critical Service Providers				
PIS	Low impact. The service is internal, automated and largely independent of external factors. The current providers are global market players.	ML	L	L
AIS	Low impact. The service is internal, automated and largely independent of external factors. The current providers are global market players.	ML	L	L

Business Impact Analysis				
Core Function	**Scenario**	**Impact**	**Probability**	**Risk**
P2PLPO Activities CPO Activities CCP Activities	Low impact. The service is internal, automated and largely independent of external factors. The current providers are global market players.	ML	L	L
EMI Activities	Low impact. The service is internal, automated and largely independent of external factors. The current providers are global market players.	ML	L	L
AML Compliance	Subcontractor management is outsourced to AMLproviders.	ML	L	L
KYC / KYB	Subcontractor management is outsourced to KYC/KYB providers.	ML	L	L

Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for the relevant business processes are specified in the table below:

	Business Process	RTO	RPO
1	Neopay PIS	4 hrs	4 hrs
2	Neopay AIS	24 hrs	4 hrs
3	EMI Activities	4 hrs	4 hrs
4	P2PLPO and CCP Activities	48 hrs	0
5	CPO Activities	48 hrs	0
6	AML Compliance	4 hrs	2 hrs
7	KYC / KYB	4 hrs	4 hrs

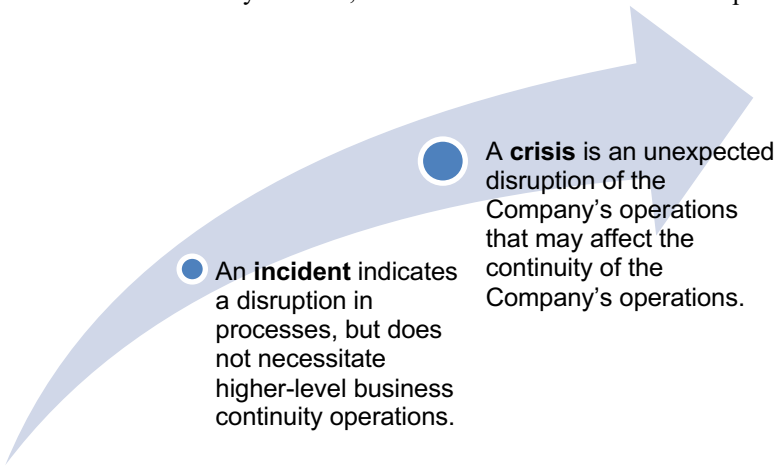
Circumstances and situations that may give rise to risks to the Companies' operations and their probability must be continuously analysed to ensure the continuity of the Companies' operations.

BUSINESS CONTINUITY CULTURE

The objective of the Companies' Business Continuity Plan is to prevent the interruption of the Companies' operations, avoid or minimise losses resulting from potential business disruptions, and restore the Companies' operations as quickly and efficiently as possible after an incident or crisis. The Companies aim to:

- Protect people's health and lives and ensure continuity of services;
- Anticipate potential incidents, crises and emergencies and assess their impact on the Companies' operations;
- Identify preventive measures for potential incidents and crises as well as measures to ensure business continuity, and plan the Company's infrastructure accordingly;
- Establish principles for managing alternative processes;
- Ensure rapid response to incidents and crises and minimise their impact on the Companies and their customers;
- Ensure effective exchange of information within the Companies, with customers, the public, key service providers and the Bank of Lithuania.

Companies recognise the seriousness of every incident, as unresolved incidents can develop into more serious disruptions/crises.



All employees of the Companies, as well as third parties with access to the Companies' information systems and information, must read and comply with the Plan.

INCIDENT MANAGEMENT AND RISK SCENARIOS

An incident or specific risk scenario may adversely affect the availability, integrity and operational security of information. This may also lead to a compromise or disruption of business continuity. Any incident can become a crisis if the impact on the Companies' operations is significant or long-lasting (longer than the RTO and RPO specified in the Business Impact Analysis for business processes).

The incidents described below constitute potential risk scenarios that could have a material impact on the Companies' business:

CRISIS MANAGEMENT

The objective of crisis management is to outline the crisis management and communication actions of the Companies to ensure immediate response to crisis situations, to manage the reputation of the Companies, and to restore the functionality of the Companies' processes quickly and efficiently. Crisis management must be escalated if the Companies' operations cannot be restored within 1 working day (24 hours), as specified in the Business Impact Analysis, or if unexpectedly high data losses are recorded.

Given that a crisis poses a serious threat to the Companies' reputation and obligations to customers and other third parties, employees must be ready to respond quickly. A clear communication plan and alternative arrangements for the Companies' activities are in place to minimise the impact of the crisis.

The Companies have developed this Plan to address the immediate demands of a crisis response where specific measures are needed for the following:

- Protecting the reputation/public image of the Companies;
- Establishing an effective Crisis Response Team, including external advisers;
- Managing direct communication and information on the organisation of alternative activities of the Companies;
- Managing the Companies' resources effectively in a crisis situation;
- Implementing measures to restore the Companies' operations as soon as possible.

The Business Process Owner shall report an incident that can trigger a crisis to the Chief Administrator and the Crisis Management Committee.

The Crisis Management Committee shall convene emergency meetings to assess and classify the crisis, to manage the overall response to the crisis, to take decisions on the mobilisation of additional resources and to approve the communication plan.

The Crisis Response Team may comprise a public relations agency and providers of outsourced functions.
Depending on the type of crisis, the Team may be assigned additional functional responsibilities:

Function	Description / Task
Safety	Safety assessment, fire safety/occupational safety issues
Information security	Assessing the security impact of the situation, advising the Crisis Management Committee, acting as a contact person for all information security issues
Technology	Assessing the technological impact of the situation, advising the Crisis Management Committee, acting as a contact person for all IT issues
Finance	Assessing financial impact, liaising with insurance companies and banks, coordinating necessary financial transactions
Risk	Assessing the impact of risk management, evaluating the overall impact of the Crisis Management Committee's decisions on the Company's future operations
Operations	Assessing the impact of the situation on the Company's operations, advising the Crisis Management Committee, acting as a contact person for all operational issues
Communication	Third-party representatives who should be included as external advisors (i.e. a public relations agency) are directly responsible for incident resolution (i.e. IT service providers)

The Crisis Management Committee shall review the affected areas of the Company's operations, evaluate the recommendations of the responsible functional units and approve the course of action.

Depending on the type of crisis, a decision should be made on alternative arrangements for the organisation of the Companies' activities.

A list of all relevant components that need to be addressed during a crisis should be reviewed.

COMMUNICATION RESPONSIBILITIES

The priority areas and responsibilities for communication are as follows:

- Every employee shall report any situations or disruptions observed to their immediate supervisor. Employees are prohibited from discussing the matter further.
- Department managers shall liaise with the Chief Administrator, Deputy Administrator, relevant providers, and coordinate with other department managers. They shall also organise alternative departmental work in crisis situations, if necessary.
- Chief Administrator or his authorised Deputy Administrator shall communicate with the Board of Directors, external providers, manage external communication, and coordinate communication with the Regulatory Authority.
- Head of Marketing and Communications (Paskolų Klubas) / Commercial Director (Neopay) / Director (Finomark) communicate with affected customers as directed by Chief Administrator or his authorised Deputy Administrator.
- Head of the Legal Department shall communicate with the Regulatory Authority and assist the Chief/Deputy Administrator in making decisions.
- Information Security Officer shall advise the Chief/Deputy Administrator on issues related to problem solving and troubleshooting.
- The Company's Board of Directors shall be kept informed of the crisis, decisions and communication.

COMMUNICATION WITH THE BANK OF LITHUANIA

The Bank of Lithuania shall be informed when the disruption thresholds specified in this table are reached.

	Major Payment-related Operational or Security Risk Incident (MOSRI)	
Level of Impact	Lower Impact Level	Higher Impact Level
Number of Criteria	**3 and >**	**1 and >**
Criteria		
1. Affected Transactions	> 10% of the Payment Service Provider's normal level of transactions (based on the number of transactions) and MOSRI duration > 1 hour [1] **or** > EUR 500 000 and MOSRI duration > 1 hour	>25% of the Payment Service Provider's normal level of transactions (based on the number of transactions) **or** > EUR 15m
2. Affected Payment Service Users	> 5 000 and MOSRI duration > 1 hour **arba** > 10% of payment service users of the Payment Service Provider and MOSRI duration > 1 hour	> 50 000 **arba** > 25% of payment service users of the Payment Service Provider
3. Service Downtime	> 2 hours	Not applicable
4. Other Payment Service Providers or Related Infrastructure Facilities That May Be Affected	Yes	Not applicable
5. Impact on Reputation	Yes	Not applicable
6. Economic Impact	Not applicable	> Max (0.1% of Tier 1 capital [2], EUR 200 000) **or** > EUR 5m
7. High-level Internal Distribution	Yes	Yes, and likely in crisis (or equivalent) mode.
8. Breach of Network and Information System Security	Yes	Not applicable

ALTERNATIVE BUSINESS OPERATIONS ARRANGEMENTS

In cases where the continuity of operations at the existing premises of the Companies is temporarily impossible but is expected to be restored, the following measures shall be taken to resolve the issue:

- If the recovery period is short, i.e. up to 48 hours, it is not justified to allocate funds for the partial or complete transfer of operations to alternative infrastructure;
- If the existing premises are not accessible, employees shall work from home.

DISRUPTION LOGGING AND REPORTING

All incidents must be recorded in the Companies' Operational or Security Risk Event/Incident Register. The employees must follow the following procedures when reporting incidents, accidental emergencies and crises, and restoring business continuity:

- In the event of an incident, the Process Owner shall take action. All disruptions are reported to all IS users, the IT Project Manager (Paskolų Klubas), the Product Manager (Neopay) and the Director (Finomark).
- Information about major Payment-related Operational or Security Risk Incident (MOSRI) shall be reported at the discretion of the Chief Administrator in accordance with the parameters set out in COMMUNICATION WITH THE BANK OF LITHUANIA, using the REGATA platform at https://regata.lb.lt/.
- All incidents related to information security must be reported to the CISO.

BUSINESS CONTINUITY PLAN REVIEW AND CONTINUOUS IMPROVEMENT

The effectiveness of control measures, communication and competences shall be reviewed once a year by testing the Plan. Responsible employees and providers shall participate in the testing. The testing scenario shall be organised by the CISO together with the Chief Administrator or his authorised Deputy Administrator.

Testing should assess the effectiveness of communication, the ability to coordinate activities in a timely and effective manner, the tools and competences available, and whether critical activities and support resources can be restored within the time specified in the Plan (RTO/RPO).

The results of the assessment should be documented. Any deficiencies should be described in as much detail as possible so that systematic improvements can be made where necessary. The elimination of identified deficiencies should be monitored regularly.

The Business Continuity Plan should be reviewed at least once a year.

The CISO shall be responsible for preparing and regularly reviewing the Business Continuity Plan, as well as for arranging the documentation of the testing and trial results.

Once the testing has been completed, the CISO, the Chief/Deputy Administrator, and the Heads of Departments shall evaluate the testing outcomes and submit the results to the Board of Directors no later than within twenty (20) working days.

FINAL PROVISIONS

The plan shall become effective upon approval by the Company's Board of Directors.

The Plan shall be revised in accordance with legislative, regulatory and organisational changes, and at least once a year.

The Plan shall be tested annually against risk scenarios.

The Heads of Departments shall be briefed on the Plan.

The Company's Director shall be responsible for the overall implementation of the Plan. The provisions of the Plan relating to information technology shall be implemented and monitored by the Heads of Departments; the provisions relating to information security shall be implemented and monitored by the CISO; and the provisions related to operational risk shall be implemented by the Risk Officer who shall further ensure appropriate controls.

APPENDIX 1. STRUCTURE AND CONTACTS OF THE CRISIS MANAGEMENT TEAM MEMBERS

[CONFIDENTIAL]

APPENDIX 2. CONTACTS OF SECURITY AND OTHER SPECIAL SERVICES AND AUTHORITIES TO BE NOTIFIED OF INCIDENTS

No	Institution	Contacts	Subject
1	Bank of Lithuania	Totorių g. 4, LT-01121 Vilnius T: +370 800 50 500	Notification of incidents that disrupt or interrupt the Bank's services
2	State Data Protection Inspectorate	L. Sapiegos g. 17, 10312 Vilnius T: +370 5 271 2804, +370 5 279 1445 E: ada@ada.lt.	Notification of incidents involving personal data breaches
2	National Cyber Security Centre	Gedimino pr. 40, Vilnius Company code 191630942 T: +370 706 84116 E: info@nksc.lt Incidents may be reported by completing a dedicated form or by emailing cert@nksc.lt or by calling 1843.	Notification of incidents occurring on public electronic communication channels and/or information systems
3	Emergency Response Centre	T: 112	Notification of breaches/incidents related to the Company's premises, other breaches/incidents that pose a threat to the Company and its employees and customers (to the Police, Fire and Rescue Service, Emergency Medical Service)

APPENDIX 3. CONTACTS OF SERVICE PROVIDERS CRITICAL TO THE CONTINUITY OF THE COMPANY'S OPERATIONS

[CONFIDENTIAL].